INFO LOG-00 MFA-00 EEB-00 AF-00 AID-00 A-00 CIAE-00
INL-00 DNI-00 DODE-00 DOTE-00 WHA-00 PERC-00 EAP-00
DHSE-00 EUR-00 OIGO-00 FAAE-00 FBIE-00 H-00 TEDE-00
INR-00 IO-00 L-00 MOFM-00 MOF-00 NEA-00 DCP-00
ISN-00 NSCE-00 OIG-00 PC-01 P-00 ISNE-00 DOHS-00
FMPC-00 SP-00 IRM-00 SSO-00 SS-00 DPM-00 USSS-00
NCTC-00 CBP-00 SCRS-00 DSCC-00 SCA-00 SAS-00 FA-00
SRAP-00 SGC-00 PESU-00 /001R

P 291659Z JUN 09
FM SECSTATE WASHDC
TO SECURITY OFFICER COLLECTIVE PRIORITY
AMEMBASSY TRIPOLI PRIORITY
INFO AMCONSUL CASABLANCA PRIORITY
XMT AMCONSUL JOHANNESBURG
AMCONSUL JOHANNESBURG

S E C R E T STATE 067105

NOFORN

E.O. 12958: DECL: MR
TAGS: ASEC
SUBJECT: DIPLOMATIC SECURITY DAILY

Classified By: Derived from Multiple Sources

SECRET//FGI//NOFORN

Declassify on: Source marked 25X1-human, Date of source: June 27, 2009

¶1. (U) Diplomatic Security Daily, June 27-29, 2009

¶2. (U) Iraq - Paragraphs 7-11

¶3. (U) Significant Events - Paragraphs 12-23

¶4. (U) Key Concerns - Paragraphs 24-43

¶5. (U) Cyber Threats - Paragraphs 44-57

¶6. (U) Suspicious Activity Incidents - Paragraphs 58-64

¶7. (U) Iraq

¶8. (S//NF) Alleged plans by various insurgent groups to conduct attacks during anticipated U.S. military withdrawal from urban areas: According to recent multiple source reports, various insurgent groups and militias intend on attacking multiple venues throughout Iraq in anticipation of U.S. military forces withdrawal from urban areas. Specific targets mentioned included the International Zone (IZ), Victory Base Complex, joint security stations, and various forward operating bases in Baghdad and in Maysan Province (southern Iraq). Allegedly, insurgent groups also are prepared to target key infrastructure, such as bridges and major supply routes used by Coalition forces (CF) and Iraqi Security Forces (ISF) convoys. According to one source, an unidentified group had access to a large tank of chlorine, 16 V-8 rockets, and three torpedoes which were supposedly recovered by the CF and ISF. The reports mentioned the attacks would commence on or about July 1. The Government of Iraq is anticipating the offensive and has placed ISF units on alert and cancelled all leave effective June 28.

¶9. (S//NF) DS/TIA/ITA would like to note the series of reports are consistent with other recent threat reporting indicating the possibility of insurgent groups and militias preparing to increase attacks in anticipation of troop withdrawal from urban areas. It is possible that extremist-affiliated groups would seek to target the IZ and the Victory Base Complex, as the venues are symbolic of the U.S. diplomatic and military presence in Iraq. It is also plausible the groups may surmise that a large attack against CF troops in these areas would be ideal, as it would serve as propaganda for them, allowing them to take credit for driving

out "occupying forces."

¶10. (S//NF) DS/TIA/ITA would also highlight the allegation of the existence of the weapons cache, as the materials could possibly be used as components for improvised rocket-assisted munitions or an improvised explosive device (IED). According to the Multi-National Forces in Iraq Combined Intelligence Operations Cell, the first documented chlorine attack occurred in al-Anbar Province (western Iraq) on October 21, 2006, and the first documented chlorine vehicle-borne IED (VBIED) in the Baghdad area occurred in Taji on February 20, ¶2007. Despite the claims by insurgent groups and militias of chlorine-related attacks, their incident rates remain low and inconsistent. While DS/TIA/ITA cannot corroborate the veracity of the recent threat reporting, overall, there is nothing to suggest that the intention to attack the U.S. presence in Iraq will subside once a military troop withdrawal is completed. (Appendix sources 1-7)

¶11. (SBU) Indirect fire (IDF) of unknown size was launched against the IZ in Baghdad at 9:22 p.m. on June 24. The IDF impacted in the river approximately 250 meters south of the U.S. Embassy compound. No injuries or damages were reported. (RSO TOC Baghdad Spot Report)

¶12. (U) Significant Events

¶13. (C) WHA Honduras - Honduran military forces arrested President Manuel Zelaya June 28 according to orders issued by the National Congress and the Supreme Court of Honduras. Zelaya was taken to a local air force base and flown to Costa Rica. Emergency Action Committee (EAC) Tegucigalpa subsequently met to discuss the ramifications of the seizure of the president by host-cost country military forces. The RSO noted the general climate in the capital was calm; however, a standfast order was issued, and additional security measures were implemented. The Embassy released a Warden Message regarding the actions against Zelaya and urged AmCits to remain in the residences or hotels for the day.

¶14. (C) Later in the day, Congress officially named Roberto Micheletti interim president. The U.S. Ambassador gave a press conference outside the Embassy; he insisted that President Zelaya was the only democratically elected president of the country and urged that freedom of expression and circulation be restored. He also demanded the release of those government officials said to be in military custody. The EAC reconvened to assess the situation. Protest activity has centered around the presidential palace, some roads in the capital were blocked, and there were some troops on the street. However, traffic flow was reported normal in most of the city. Authorized Departure for family members was discussed, but not warranted at this time. Embassy personnel were advised to remain in their homes for the rest of the day and to limit their movements today, June 29. All Peace Corps volunteers have been accounted for and are on standfast. Post will be open today for emergency services only. The EAC will continue monitoring events in-country and provide updated information as available. (Tegucigalpa Spot Report; telcon; Warden Message; Appendix sources 8-10)

¶15. (SBU) EUR Germany - A Local Guard Force (LGF) member of U.S. Consulate General Frankfurt discovered two suspicious cases with protruding wires June 26 while on foot patrol in the clustered housing area. The guard notified his supervisor, and the area and two nearby apartment buildings were evacuated. Responding police requested canine and Explosive Ordnance Disposal (EOD) support. After the EOD team arrived, a local telecom technician, who had been working nearby, arrived at the scene and claimed the unattended cases; the technician had inadvertently left the cases. After further investigation and corroboration with the technician, police declare the area safe. (RSO Frankfurt Spot Report)

¶16. (SBU) AF Liberia - Two acts of vandalism were reported to U.S. Embassy Monrovia on the night of June 27. One took place at the residence of the chief of the DoD Office of Security Cooperation, approximately 2.5 miles from Post, where

graffiti was spray painted on the perimeter wall stating, "COL THE WAR HAS JUST BEGAN." The second incident occurred at the facility of a USAID-funded project, approximately 1.5 miles from the Embassy, where the messages "INTERCON MUST LEAVE NOW, TAKE INT" and "DANGER" were spray painted on the compound wall. The RSO assesses these incidents are consistent with the pattern of threats and intimidation used by dismissed Embassy guards to obtain a favorable settlement with their former employer through the Liberian Ministry of Labor. (RSO Monrovia Spot Report)

¶17. (SBU) Mauritania - U.S. Embassy Nouakchott received a credible threat June 27 regarding a kidnapping against an American in the capital sometime during the night (NFI). The RSO considers the information credible and made notifications to staff to assure that all official Americans were accounted for. All residential LGF posts were manned, and radio checks were increased. Post also issued a Warden Message advising AmCits in-country of the threat. Please see the Key Concerns section for further information. (RSO Nouakchott Spot Report)

¶18. (C//NF) Mauritania - EAC Nouakchott met June 26 to discuss developments surrounding the murder of an unofficial American on June 23. Members were updated on the investigative progress of local authorities. The EAC reviewed the U.S. Embassy's tripwires for consideration of Authorized Departure and/or drawdown and determined there was insufficient information at this time to recommend either action. EAC members were reminded of the importance of random arrival arrivals at Post (effective June 25) along with other augmented security measures.

¶19. (S//NF) The EAC reconvened June 28, and members were introduced to FBI assets assigned to investigate the AmCit's murder with host-country law enforcement personnel. Members welcomed the team and support their efforts on the investigation while in-country. Members also discussed the credible kidnapping threat against an AmCit in-country and reviewed the enhanced security measures already in place. Post issued a Consular short message system alert to the American community advising of the threat. The EAC will continue to review all threat information as it becomes available, while supporting the ongoing murder investigation, and the EAC will reconvene as needed. (Appendix sources 11-12)

¶20. (SBU) Sudan Update - On June 24, verdicts were issued in the trial of the five Sudanese men charged with the January 1, 2008, murder of U.S. Embassy Khartoum employees John Granville and Abdelrahman Abbas. Four of the defendants were found of guilty of intentional killing and sentenced to death by hanging. The fifth defendant was found guilty on weapons charges and sentenced to two years in prison, including credit for time served since his January 2008 arrest. (Khartoum 0790)

¶21. (SBU) The Gambia - EAC Banjul met June 23 for its monthly meeting. It was determined that the recent activity in Tehran, Iran, should not present any additional danger for U.S. personnel or citizens in-country; however, the EAC agreed U.S. Embassy staff must be more diligent in practicing common-sense security measures. EAC members deemed Post's current security posture is sufficient. (Banjul 0190)

¶22. (S//NF) NEA Yemen - EAC Sana'a met June 28 to discuss a write-in threat concerning a VBIED attack against the U.S. Embassy planned for today, June 29. The threat was traced to Algeria, and, although such threats are considered relatively common, Post officials are taking the threat seriously. Members agreed that Post's current security upgrades were sufficient to deter and, if need be, withstand an attack; however, members deemed it would be prudent to request additional security from the Republic of Yemen Government at Post's perimeter, in light of the approaching July 4 holiday. Please see the Key Concerns section for further details. (Appendix source 13)

¶23. (C) SCA Bangladesh - U.S. Embassy Dhaka officials met with the secretary of Home Affairs to discuss concerns over

an uptick in crimes directed against foreigners in Dhaka's Diplomatic Enclave. The secretary stated the Government of Bangladesh (GoB) had increased the police presence in the enclave May 7, when threat letters were sent to several diplomatic missions. Post officials will continue to monitor the situation and keep pressure on the GoB to provide adequate security to the U.S. Mission. (Appendix source 14)

¶24. (U) Key Concerns

¶25. (S//NF) AF Mauritania - AQIM threat to kidnap American citizen: According to the Spanish National Intelligence Service (CNI), an unidentified source for the CNI service center stated al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) planned to kidnap an unidentified AmCit in Nouakchott during the evening of June 27. According to the report's context statement, a CNI official provided the information during the course of a routine liaison meeting. There are no additional details on this information, and the report's originators are unable to assess the reliability of the ultimate source(s) of the information. In addition, it is not known what, if any, vetting or validation procedures the Spanish service may use to evaluate its sources. In separate reporting, AQIM, as of late June, had sent three unidentified members to Mauritania from northern Mali to conduct operations against government interests in Nouakchott and Nouadhibou, according to the Mauritanian External Intelligence Service. It was unknown, according to the Mauritanian service, whether AQIM intended to attack Mauritanian and/or foreign government facilities in those cities. Separately, AQIM Tariq Ibn Ziyad battalion leader 'Abd al-Hamid (Abu Zaid), as of late June, had delayed an order for four men to travel to Nouakchott to conduct unspecified operations, according to the Mauritanian service. DS/TIA/ITA notes the latest threat information follows last week's killing of an American in Nouakchott and the possible involvement of AQIM. (Appendix sources 15-16)

¶26. (S//NF) Nigeria - Extremists believed to be planning a massive terrorist attack: (S//REL TO USA, FVEY) Tearline states, "Unspecified extremist groups, suspected to be operating in concert with Nigerian Shi'ites, Salafiya, or Muhammad Yusuf's Nigerian Taliban are reportedly planning to launch a massive surprise attack on some piece of critical infrastructure or against high-profile targets within Nigeria. Probable targets of this attack include top Nigerian Government officials or security agents. Members of the general public, who might be opposed to the attackers' doctrines, were also believed to be possible targets. This planned attack is reportedly aimed at sparking sectarian clashes across Nigeria."

¶27. (S//NF) DS/TIA/ITA cannot immediately corroborate the current threat with additional intelligence. While no connection can be made between this threat and previous reports, DS/TIA/ITA is concerned about recent activity surrounding extremists associated with the Nigerian Taliban.

¶28. (S//NF) A well-trained veteran Chadian extremist, Abu-Mahjin (Terrorist Identities Datamart Environment (TIDE) number 24350378), who has limited ties to al-Qa'ida associates, recently traveled to Nigeria. He may be planning to conduct or facilitate a terrorist operation. Indeed, tearline from May 1 claimed, "An Islamic extremist named Abu-Muhjin has recently been in northeast Nigeria. It is likely that he will be joined by other Islamic extremists in the coming weeks." More recent tearline stated, "Nigerian-based probable Chadian extremist Abu-Mahjin is keen to obtain more funds in connection with some sort of nefarious activity (possibly terrorism related) he is engaged in. However, it is not clear when he will receive this additional finance." Little more is known about Abu-Mahjin's apparent efforts to organize a near-term operation.

¶29. (S//NF) Though neither the Nigerian Taliban nor its more militant subset -- Tanzim al-Qa'ida group -- has ever attacked Western interests, they have discussed targeting foreign embassies in the past. In 2007, they reportedly

plotted to attack the U.S., British, and Israeli embassies in Abuja, according to a single source that remains unsubstantiated. (Appendix sources 17-19)

¶30. (C//NF) NEA Algeria/Yemen - Unsubstantiated threat claiming suicide bombing against U.S. embassies: On June 26, a write-in to a USG website provided a message involving an unsubstantiated threat to U.S. embassies in Algiers, Algeria, and Sana'a, Yemen. The message was posted in Arabic and appeared to originate in Algeria. The writer warned of a "big attack against your embassies in Algeria and Yaman by suicide car on 29/06/2009" and claimed to be an agent of the Algerian Intelligence Service. The writer provided an apparent telephone number for confirming his information and warned, "The second attack what you will see it is in Hassi Messaud in Sahara by a big number of terrorists." The report's originators note that they have no further information to corroborate the information, and the source may have intended to annoy, mislead, or disrupt rather than to provide legitimate information. The originators further note that the vast majority of such information is not true, but, since volunteers have provided authentic leads on occasion, the information is provided for evaluation purely due to its threat content. (Appendix source 20)

¶31. (S//NF) Yemen - Al-Qa'ida possibly planning Embassy attacks: (S//REL TO USA, FVEY) According to tearline information, "Saudi authorities learned in late June that al-Qa'ida may be planning an attack on Western and Middle Eastern embassies in Yemen. There was no additional information on the timing or exact location of the planned attack."

¶32. (S//NF) DS/TIA/ITA notes this report is likely related to recent information provided by a Yemeni security official in late June regarding possible unspecified al-Qa'ida in the Arabian Peninsula (AQAP) attacks against the embassies of the U.S, Qatar, United Arab Emirates, Oman, Saudi Arabia, and unnamed European nations in Sana'a. No further information was provided on this general threat report.

¶33. (S//NF) DS/TIA/ITA also notes the continuing AQAP threat to Western and host-nation interests both in Sana'a and throughout Yemen. Previous AQAP attacks illustrate a willingness and capability to target Western citizens and diplomatic facilities, highlighted by the brazen attack against U.S. Embassy Sana'a in mid-September 2008. The lack of host-nation political will to combat AQAP contributes to an extremely permissive operating environment for extremist elements, suggesting threat reporting against U.S. and other foreign interests in Yemen will continue in both the near and medium term. (Appendix sources 21-22)

¶34. (S//NF) SCA Afghanistan - Threat to unspecified American in Kandahar: As of late June, Kandahar Taliban members Sadiq, Mullah Hamdullah, and Qari Yousef intended to kidnap an unspecified American who travels from Kandahar Airfield to work in Kandahar city to hold for ransom. The kidnappers planned to use a local Afghan who the American trusted to place a substance in his food to render him unconscious. Hamdullah, a.k.a. Bari Alai, worked under the command of Mullah Faizel who was currently in detention at Guantanamo Bay.

¶35. (S//NF) While the Taliban operatives named in this report are indeed active in and around Kandahar city to include involvement in kidnapping plots, DS/TIA/ITA questions the source's access to operational plans by the Taliban. In past reporting, the source has reported primarily on Taliban member atmospherics and movements in southern Afghanistan and only occasionally on threats. DS/TIA/ITA assesses information provided by the source regarding the January 2008 kidnapping of an American non-governmental organization (NGO) worker to be inaccurate.

¶36. (S//NF) That said, periodic reporting indicates extremists remain keen to abduct another Westerner in Kandahar city, possibly while traveling to/from Kandahar

Airfield. Tearline states, "Taliban insurgents reportedly planned in late January to kidnap a U.S. national as he traveled between Kandahar Airfield and Shur Andam Pass, Kandahar Province." Reporting from November 2008 alleged the Taliban planned to kidnap two foreign women possibly from their residence in northeast Kandahar city or at the Rang Rezano market they frequented.

¶37. (S//NF) Mullah Faizel (variants: Faisal, Fazilfazul; TIDE number 72569) was being held at Guantanamo Bay as of early April 2008. Mullah Hamdullah (possible TIDE number 75483) is characterized in late-2008 sensitive reporting as a group commander of a large number of Taliban in Helmand Province. The same report noted Sadiq, the brother of the Taliban's second-in-command Mullah Berader (TIDE number 76541), worked at an unnamed U.S. NGO and was involved in planning an unspecified kidnapping. (Appendix sources 23-30)

¶38. (S//FGI//NF) Pakistan - Militants may be planning to abduct U.S. and UK citizens from NGOs and consulates; dual-citizens in Peshawar: Tearline intelligence reports, "Militants attached to Pakistan's Mumtaz Group may be planning to kidnap U.S. and UK citizens working in NGOs and consulates, as well as dual-citizen Pakistanis who are either visiting or residing in Peshawar, as of June 26. Peshawar's University Town could be the likely venue for such an operation. Further, the following individuals who probably reside in (the) Peshawar area could be supporters of the Mumtaz Group: Fahim, son of Ihsanullah; Ayaz; Abdul Rehman Khan (Awami National Party) and his son, Yunas Khan, residents of Kafir Dheri, Peshawar; Garib Shah Badshah; and Muazzam Badshah, son of Shah Badshah."

¶39. (S//FGI//NF) DS/TIA/ITA assesses the Mumtaz Group may be a reference to operations linked to al-Qa'ida leader Hamza al-Jawfi (a.k.a. Mumtaz; TIDE number 70390) who died in a late-February explosion in North Waziristan. Mumtaz is an oft-used alias by senior al-Qa'ida leaders that is arguably inauspicious. The now-deceased Hamzah Rabi and Abu Khabab al-Masri both used this alias as well. Worryingly, the other operatives DS/TIA/ITA suspects belong to this group are linked to ongoing, credible planning against Peshawar cantonment as well as American personnel and convoys belonging to U.S. Consulate Peshawar.

¶40. (S//FGI//NF) Although al-Jawfi is dead, it is possible the operations referenced can be linked to al-Jawfi's former courier and Imran (TIDE number 14399906), who collaborates closely with Mohmand Agency-based Tehrik-e-Taliban Pakistan (TTP) commander Hakimullah Mahsud. Early-April reporting from Inter-Services Intelligence (ISI) links Imran -- described as an Uzbeki militant responsible for the November 12, 2008, murder of a USAID contractor and the August 26, 2008, ambush of the principal officer's (PO's) vehicle in Peshawar -- to TTP operative Faruq's ongoing planning for an attack on Peshawar's cantonment using multiple suicide operatives. Faruq is also likely involved in conducting al-Qa'ida-linked operational surveillance against the PO of U.S. Consulate Peshawar, a four-vehicle SUV protective convoy, and a vehicle workshop also affiliated with Post. Of note, however, ISI reported the capture of an individual named Imran in mid-June; although, it cannot be confirmed if this is the same Uzbeki Imran mentioned in earlier reporting. (Appendix sources 31-38)

¶41. (S//FGI//NF) Pakistan - Threats against Punjab and Islamabad: Reporting continues to circulate detailing ongoing plans by Pakistani extremists to launch suicide operations in Punjab Province and Islamabad. In Islamabad, threats specify the targeting of embassies located in the F-6/2 sector, police post Aabpara in Islamabad, the Imam Bargah in G-6/2, Senator Tariq Azim, and Barri Imam Shrine. In Lahore and greater Punjab Province, suicide operatives may seek to strike against foreigners in crowded areas or the Barbar Data Sahib Shrine. Although it remains unclear if these named targets are an accurate reflection of extremists' operational plans, it is of note late-June reporting also mentions the cultivation and use of sympathetic madrassas and extremists

located in targeted cities to carry out future attacks.

¶42. (S//NF) As of late June, TTP reportedly tasked Abdul Malik Mujahid to launch suicide attacks against unspecified foreigners in crowded places in Punjab, with Mujahid considering the use of sympathetic madrassas as shelter prior to conducting an attack. Madrassas under consideration included the Jami Ashrafia and Jamiat ul-Manzur ul-Islami in Lahore. Separately, tearline from late June reports, "Militant commander Khan Bahadur, son of Sher Bahadur, is the local militant commander in the Watkai area. Bahadur currently may be residing in Islamabad, while reorganizing his group to operate in difference parts of Pakistan, as of June 25." Although there is limited information regarding the identity of Khan Bahadur (possible TIDE number 238258), earlier sensitive intelligence suggests he has served as an interlocutor in urban areas for Waziristan-based militants since 2007. According to late-January 2008 tearline, "... A Khan Bahadur (or Bhadur) in Lahore was involved in efforts to arrange talks and perhaps a government announcement for a cease-fire and helping coordinate a separate announcement from the Mujahidin, hopefully by October 13...."

¶43. (S//FGI//NF) As underscored by the events during and following the Lal Masjid (Red Mosque) confrontation in Islamabad in July 2007, the continued existence of networks in Islamabad that can organize and facilitate protests and terrorist activity in the vicinity of the capital is indeed troubling. Notably, a body of intelligence reporting preceding the Lal Masjid confrontation suggests Pakistan-based extremists viewed the brewing tension between the madrassas and Islamabad one part of a larger comprehensive effort to re-energize and expand their jihadi operations from their strongholds in the tribal areas and Northwest Frontier Province. Interestingly, reporting from May 2007 citing a commander 10 corps lieutenant also noted 70 mosques in and around Islamabad would likely support extremist activity associated with the now-infamous Lal Masjid, which was also an unauthorized mosque. Of concern, since 2008 attacks in Pakistan have repeatedly targeted Westerners, coinciding with an unprecedented number of attacks in both Lahore and Islamabad. (Appendix sources 39-47)

¶44. (U) Cyber Threats

¶45. (U) EUR CTAD comment: The latest version of the National Security Strategy released by the UK Government includes a public cyber security strategy. The report calls for the establishment of two new offices with cyber security responsibilities and approves the use of offensive operations as a countermeasure to attacks against British systems. The Office of Cyber Security, falling under the Cabinet Office, will be the central body charged with coordinating with industry and developing strategy. The Cyber Security Operations Centre based at Government Communications Headquarters, the UK's primary signals intelligence agency, will be responsible for conducting offensive operations. According to press reports, the UK Government has hired several former hackers to staff the centre.

¶46. (S//NF) NEA CTAD comment: DoD reporting indicates as of mid-May, several Persian-language hacker forums are sharing information pertaining to a variety of hacking codes, tools, and video tutorials. One of the more notable findings was a PHP-based "simattacker code" -- a backdoor Trojan horse program that allows for remote exploitation of an affected system and can provide denial-of-service capabilities. This particular malicious code is reportedly similar to a tool used against Georgian systems in 2008 (NFI).

¶47. (SBU) EAP CTAD comment: According to South Korean press reporting, the Republic of Korea's (RoK's) Defense Security Command (DSC) has declared intrusion attempts against the RoK's military computer networks have increased 20 percent in 2009, compared to those detected in 2008. The DSC further stated that 89 percent of the attempts are unsophisticated efforts to hack into servers and Internet homepages, whereas the remaining 11 percent appear to be more advanced attempts

to obtain intelligence information. Of note, in an effort to deal with the increasing cyber threat, the RoK's National Intelligence Service has recommended President Lee Myung-bak appoint an aide to assist with the country's cyber security issues.

¶48. (S//NF) SCA CTAD comment: According to Defense Intelligence Agency reporting, the Government of India (GoI) continues efforts to advance its computer security programs -- particularly in light of increased concerns over Chinese computer network exploitation efforts -- but progress is hampered by significant disagreements within its departments. The key GoI organizations involved in developing and implementing security policies are identified as the Ministry of Telecommunications and the Research and Analysis Wing. Although the Indian Army is primarily responsible for the security of military networks, Indian officials acknowledge Army representatives have been largely left out of discussions. Additionally, some other key groups, such as the National Technical Reconnaissance Organization and the Indian Defense Intelligence Agency, have reportedly failed to offer significant contributions. Private security companies are also concerned that the lack of input from the private sector may lead to unfair regulations regarding telecommunications monitoring.

¶49. (SBU) Domestic CTAD comment: On June 22, Websense Security Labs issued an alert after discovering the official website of the Embassy of Ethiopia in Washington, DC, had been subverted with obfuscated JavaScript code hidden in an inline frame (IFrame) with the goal of infecting visitors to the site with malicious software (malware). The code redirected users to sites where malware, including Trojan downloaders, were installed without explicit user action. According to the alert, the site that hosted the malicious JavaScript is currently down. On March 20, security company Sophos discovered a similar IFrame infection on the same website. At the time, researchers at Sophos noted it resembled the attack on the Washington, DC, Embassy of Azerbaijan website that occurred in early March. The researchers also indicated the redirected sites had been used by Russian cyber criminals in previous malware infections. (Appendix sources 48-50)

¶50. (C) EAP China - Beijing TOPSEC founder indicates PRC investment:

¶51. (S//NF) Key highlights:
o Founder of TOPSEC and iTrusChina notes PRC funding and directive in media interview.
o TOPSEC is China's largest provider of information security products and services.
o TOPSEC provides services and training for the PLA and has recruited hackers in the past.
o Potential linkages of China's top companies with the PRC illustrate the government's use of its "private sector" in support of information warfare objectives.

¶52. (SBU) Source paragraph: "During an interview with journalists from China News Network, chairman of both Beijing TOPSEC and iTrusChina, He Weidong, spoke about the two companies, to include investment and contract from the Chinese Government (People's Republic of China (PRC)) .... Tianrongxin's capital came from two parts. The Chinese Government share one part of the investment, and the management department (of Tianrongxin) share the other part. He further stated that Tianrongxin was not really a company but a research institute; in 1995, the company took contracts from the government's research and development tasks."

¶53. (S//NF) CTAD comment: In November 1995, He Weidong founded the security company Tianrongxin, a.k.a. Beijing TOPSEC Network Security Technology Company, Ltd. TOPSEC is a China Information Technology Security Center (CNITSEC) enterprise and has grown to become China's largest provider of information security products and services. TOPSEC is credited with launching China's first indigenous firewall in 1996, as well as other information technology (IT) security

products to China's market, to include virtual private networks, intrusion detection systems, filtering gateways, and security auditing and management systems. Additionally, in September 2000, Weidong founded the company Tianweichengxin, a.k.a. iTrusChina, which became the first experimental enterprise to develop business Public Key Infrastructure/Certification Authority services approved by China's Ministry of Industry and Information Technology.

¶54. (SBU) CTAD comment: During an interview with China News Network, Weidong stated that half of TOPSEC's start-up capital came from the PRC, with the other half coming from the company's management department. Additionally, he pointed out that TOPSEC began not as a company, but as a small research institute that took contracts from the government's research and development tasks (NFI). The turning point for TOPSEC came in 1996 when the company won a significant contract bid from the Chinese State Statistics Bureau. Since winning the bid, TOPSEC maintained a 100-percent sales growth in the following years. Weidong noted the company started out with 30,000 RMB (approximately $4,400) in 1995, and by 2002, had earnings of 3 billion RMB (approximately $440,000,000). Interestingly, shareholders did not receive bonuses, as all earnings went for future investment. Weidong also stated a bank loan was never used.

¶55. (S//NF) CTAD comment: Of note, the CNITSEC is responsible for overseeing the PRC's Information Technology (IT) security certification program. It operates and maintains the National Evaluation and Certification Scheme for IT security and performs tests for information security products. In 2003, the CNITSEC signed a Government Security Program (GSP) international agreement with Microsoft that allowed select companies such as TOPSEC access to Microsoft source code in order to secure the Windows platform. XXXXXXXXXXXX

¶56. (S//NF) CTAD comment: Additionally, CNITSEC enterprises has recruited Chinese hackers in support of nationally-funded "network attack scientific research projects." From June 2002 to March 2003, TOPSEC employed a known Chinese hacker, Lin Yong (a.k.a. Lion and owner of the Honker Union of China), as senior security service engineer to manage security service and training. Venus Tech, another CNITSEC enterprise privy to the GSP, is also known to affiliate with XFocus, one of the few Chinese hacker groups known to develop exploits to new vulnerabilities in a short period of time, as evidenced in the 2003 release of Blaster Worm (See CTAD Daily Read File (DRF) April 4, 2008).
¶57. (S//NF) CTAD comment: While links between top Chinese companies and the PRC are not uncommon, it illustrates the PRC's use of its "private sector" in support of governmental information warfare objectives, especially in its ability to gather, process, and exploit information. As evidenced with TOPSEC, there is a strong possibility the PRC is harvesting the talents of its private sector in order to bolster offensive and defensive computer network operations capabilities. (Appendix sources 51-52)

¶58. (U) Suspicious Activity Incidents

¶59. (SBU) EUR Iceland - A man and a woman photographed in the area north of U.S. Embassy Reykjavik June 25. They then walked toward the backside of the Post, where they took additional photographs before departing on foot. The man was seen photographing in the neighborhood for an additional 3 hours. The Surveillance Detection Team found it unusual the subjects photographed sites other than tourist attractions. (SIMAS Event: Reykjavik-00257-2009)

¶60. (SBU) AF Guinea - Two young men were photographed U.S. Embassy Conakry June 25. A gendarme stopped the pair and took them to a nearby security booth where they were interviewed by Post's foreign security national investigator. Their photos of the Embassy were deleted, and the subjects were released with a warning.

¶61. (SBU) Record Check/Investigation: Subject 1: Mamdou Mouminatou Diallo. XXXXXXXXXXXX Labe, Guinea. Cell phone

number: XXXXXXXXXXXX Subject 2: Mamadou Diallo. XXXXXXXXXXXX Koundara, Guinea. Cell phone number: XXXXXXXXXXXX (SIMAS Event: Conakry-01492-2009)

¶62. (SBU) NEA Tunisia - A man sat at Marsaoul Caf in Tunis focusing on the road leading to the U.S. Ambassador's residence June 4. After 30 minutes, the subject got into his car and departed the area. The man was previously seen at the caf on May 15 for approximately 1 hour.

¶63. (SBU) RSO Action/Assessment: The caf is located at the foot of the hill near the Ambassador's residence (the residence is located at the end of the road, approximately one-quarter to one-half mile away). This is the second time the individual and vehicle were spotted. However, Tunisian police do not share information concerning routine traffic stops or suspicious persons questioned/seen near the Embassy or Ambassador's residence. If the vehicle is seen again, the RSO will attempt to retrieve information on the owner.

¶64. (SBU) Record Check/Investigation: Vehicle: Gray Volkswagen; License plate: 8020TU97. (SIMAS Event: Tunis-02054-2009)

SECRET//FGI//NOFORN

Full Appendix with sourcing available upon request.
CLINTON